Séminaire Dubreil.
Algèbre et théorie
des nombres

Jean-Claude Petit

Sur certains quasi-corps généralisant un type d'anneau-quotient

Séminaire Dubreil. Algèbre et théorie des nombres, tome 20, n° 2 (1966-1967), exp. n° 13, p. 1-18

<http://www.numdam.org/item?id=SD_1966-1967__20_2_A2_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
20e année, 1966/67, n° 13

13 mars 1967

SUR CERTAINS QUASI-CORPS GÉNÉRALISANT UN TYPE D'ANNEAU-QUOTIENT

par Jean-Claude PETIT

Introduction. - La théorie des polynômes non commutatifs à une variable (voir [5] pour un exposé de cette théorie) permet de définir, et d'étudier, des anneaux à multiplication non nécessairement associative qui généralisent les anneaux-quotient d'anneaux de polynômes. Pour tout anneau de polynôme A et tout polynôme $m \in A$, on définit deux structures A/Am et A/mA dans lesquelles on a toutes les propriétés d'un anneau, sauf éventuellement l'associativité de la multiplication. On a cependant l'existence de propriétés d'associativité restreinte caractéristiques. Dans A/Am, l'étude des équations en x : $a.x = b$ et $x.a = b$ est liée à la factorisation de m dans A, et elle permet de caractériser une nouvelle classe de quasi-corps distributifs, c'est-à-dire d'anneaux à multiplication associative ou non, dans lesquels les éléments non nuls constituent une boucle multiplicative. Ceux de ces quasi-corps, dont la multiplication est associative, sont des corps gauches, et parmi les corps gauches de dimension finie sur leur centre, on donne une caractérisation de ceux qui s'obtiennent par constructions successives d'anneaux-quotient A/Am à partir d'un sous-corps commutatif maximal, pour m de la forme $x^n - a$.

1. Algèbres A/Am et A/mA.

Rappelons quelques résultats de la théorie des polynômes non commutatifs de ORE (voir [5]) :

K désignant un corps commutatif ou non, soit P l'ensemble des polynômes à coefficients dans K à une indéterminée x de la forme

$$a = \sum_{i=0}^{i=n} a_i x^i , \qquad \forall\, i , \quad a_i \in K .$$

P peut être muni de façon évidente d'une structure d'espace vectoriel à gauche sur K, avec pour base x^i, $i \in N$, en notant $x^0 = 1$. Pour avoir dans P une multiplication qui en fasse un anneau où le degré d'un produit soit égal à la somme des degrés des facteurs, il est nécessaire d'avoir :

$$\forall\, a \in K , \qquad xa = \sigma(a)x + \delta(a) ,$$

où σ est un homomorphisme injectif de K dans lui-même, et où δ est une σ-

dérivation de K , c'est-à-dire une application de K dans K vérifiant

$$\forall\, a\,,\ \forall\, b \in K\,, \qquad \delta(a+b) = \delta(a) + \delta(b)\,, \quad \delta(ab) = \sigma(a)\,\delta(b) + \delta(a)b\ .$$

Il en résulte alors :

$$x^n\, a = \sum_{p=0}^{p=n} S_{n,p}(a)\, x^{n-p}\ ,$$

avec $S_{n,0}(a) = \sigma^n(a)$, $S_{n,n}(a) = \delta^n(a)$, et $S_{n,p}(a)$ désignant la somme des C^p_{n+p} termes obtenus en considérant l'image de a par le polynôme en δ et σ , dont chaque monôme est de degré $n-p$ en σ et p en δ , deux monômes différant par l'ordre de leurs facteurs (exemple : $S_{2,1} = \sigma^2 \circ \delta + \sigma \circ \delta \circ \sigma + \delta \bullet \sigma^2$).

Réciproquement, on montre que, pour tout triple $(K\,,\ \sigma\,,\ \delta)$, où K est un corps commutatif ou non, σ un homomorphisme injectif de K dans K , δ une σ-dérivation de K , on donne à P une structure d'anneau $K[x\,,\ \sigma\,,\ \delta]$ en définissant $x^n\, a$ par les formules ci-dessus. Nous noterons simplement A cet anneau, lorsque nous supposerons fixé le choix de $(K\,,\ \sigma\,,\ \delta)$. Dans A , on dispose d'une division euclidienne à droite : $\forall\, a \in A$, $\forall\, b \in A$, il existe un couple d'éléments q et r unique vérifiant

$$a = qb + r \qquad \text{avec} \quad r = 0 \quad \text{ou} \quad d^o\, r < d^o\, b\ .$$

Il faut et il suffit que σ soit surjectif pour avoir l'existence d'une division à gauche analogue.

Définition de A/Am . - Choisissons un polynôme m dans A . Désignons par Am l'ensemble des multiples à gauche de m . Soit A_n le sous-groupe additif de A engendré par les polynômes de degré strictement inférieur à n . Si $\bar{a}$ désigne la classe de $a \in A$, modulo Am , et si r désigne le reste de la division à droite de a par m , en posant $i(\bar{a}) = r$, on définit un isomorphisme i du groupe A/Am sur A_n . Lorsque Am est un idéal bilatère, on obtient la structure d'anneau-quotient A/Am en définissant la multiplication par $\bar{a}\bar{b} = \overline{ab}$, qui s'écrit alors aussi $\bar{a}\bar{b} = \overline{i(\bar{a})\ i(\bar{b})}$. En transportant cette structure sur A_n à l'aide de i , on obtient dans A_n la multiplication définie par

$$i(\bar{a}).i(\bar{b}) = i(\bar{a})\ i(\bar{b}) - qm\ ,$$

où q est déterminé par la condition $i(\bar{a}).i(\bar{b}) \in A_n$.

DÉFINITION. - On désigne par A/Am la structure algébrique obtenue en munissant A_n de l'addition de A et de la multiplication, définie par

$$\forall\, a \in A_n\,, \quad \forall\, b \in A_n\,, \qquad a.b = ab - qm\ ,$$

où q est l'unique élément de A tel que $ab - qm \in A_n$.

Lorsque σ est surjectif, on utilise la division euclidienne à gauche pour définir A/mA avec $a.b = ab - mq$.

On peut établir le résultat suivant :

(1) A/Am a les propriétés d'un anneau unitaire, sauf éventuellement l'associativité de la multiplication.

A/Am a une structure d'espace vectoriel à gauche sur K de base x^j : $0 \leqslant j \leqslant n-1$.

A/Am est un anneau si, et seulement si, Am est un idéal bilatère de A .

Lorsque σ est surjectif, si $A = K[x , \sigma , \delta]$ et $B = {}^{0}K[x , \sigma^{-1} , - \delta \circ \sigma^{-1}]$, ${}^{0}K$ désignant le corps opposé de K , A/mA et B/Bm sont anti-isomorphes.

Prouvons, par exemple, que l'associativité de la multiplication entraîne que Am est idéal bilatère :

Si la multiplication est associative, on a :

$a.(b.c) = a(bc - rm) - sm$, avec $bc - rm \in A_n$ et $a(bc - rm) - sm \in A_n$,

$(a.b).c = (ab - pm)c - qm$, avec $ab - pm \in A_n$ et $(ab - pm)c - qm \in A_n$.

L'associativité entraîne l'égalité :

$$pmc = (ar + s - q)m \quad .$$

Choisissons alors a et b tels que $d^o\, a + d^o\, b = d^o\, m = n$, il en résulte $d^o\, p = 0$ puisque p est le quotient de la division à droite de ab par m . On peut alors se ramener au cas où $p = 1$, il suffit pour cela de remplacer a par $p^{-1}\, a$. Il vient, $\forall\, c \in A_n$, $mc \in Am$.

Si on a $d^o\, c \geqslant n$, on a

$$c = gm + h , \qquad \text{avec } h \in A_n ,$$

mais d'après la propriété précédente, il existe $k \in A$ avec $mh = m(c - gm) = km$, soit $mc = (mg + k)m$. On obtient donc,

$$\forall\, a \in A , \quad \forall\, b \in A , \qquad amb \in Am ,$$

ce qui établit que Am est un idéal bilatère.

Dans le cas où A/Am n'est pas un anneau, sa multiplication possède toutefois des propriétés intéressantes. Notons $[a , b , c] = (a.b).c - a.(b.c)$, et posons les définitions suivantes :

Noyau d'associativité à gauche :

$$N_g = \{a \; ; \quad a \in A/Am \; , \quad \forall\, b \in A/Am \; , \quad \forall\, c \in A/Am \; , \quad [a \; , \; b \; , \; c] = 0\} \; .$$

Noyau d'associativité central :

$$N_c = \{b \; ; \quad b \in A/Am \; , \quad \forall\, a \in A/Am \; , \quad \forall\, c \in A/Am \; , \quad [a \; , \; b \; , \; c] = 0\} \; .$$

Noyau d'associativité à droite :

$$N_d = \{c \; ; \quad c \in A/Am \; , \quad \forall\, a \in A/Am \; , \quad \forall\, b \in A/Am \; , \quad [a \; , \; b \; , \; c] = 0\} \; .$$

On peut établir les résultats suivants :

(2) Si A/Am n'est pas un anneau, on a

$$N_g = N_c = K \qquad \text{et} \qquad N_d = \{k \; ; \quad mk \in Am\} \; ,$$

$$d^\circ\, a + d^\circ\, b < n \implies [a \; , \; b \; , \; c] = 0 \; .$$

Effectuons, par exemple, la détermination de N_g : avec les notations utilisées plus haut, on a

$$[a \; , \; b \; , \; c] = 0 \iff pmc = 0 \; .$$

En remarquant que $d^\circ\, a = 0$ implique $p = 0$, on obtient $K \subset N_g$. D'autre part, s'il existe $a \in N_g$ avec $d^\circ\, a \geqslant 1$, choisissons b tel que $d^\circ\, a + d^\circ\, b = n$, il en résulte $d^\circ\, p = 0$, et alors

$$pmc \in Am \implies mc \in Am \; ,$$

et on en tire aisément $AmA \subset Am$, ce qui prouve que Am est un idéal bilatère.

Proposons-nous de donner des propriétés caractérisant les structures A/Am parmi les anneaux à multiplication non nécessairement associative. On obtient ainsi :

(3) Pour un anneau B à multiplication non nécessairement associative, il y a équivalence entre les trois propriétés suivantes :

(a) B vérifie 1°, 2°, 3° ;
(b) B vérifie 1°, 2°, 4°, 5°, 6° ;
(c) B est isomorphe à A/Am , avec

$$A = K[x \; , \; \sigma \; , \; \delta] \; , \qquad m = \sum_{p=0}^{n-1} m_p \, x^p \; ,$$

où σ et δ sont définies par :

$$\forall\, a \in K \; , \qquad x \star a = \sigma(a) \star x + \delta(a) \; ,$$

$\star$ symbolisant la multiplication de B, et où, dans B, on a

$$x^n = \sum_{p=0}^{n-1} m_p \star x^p , \qquad \text{avec } x^0 = 1 \text{ et } x^{p+1} = x \star x^p \text{ pour } 0 \leqslant p \leqslant n-1 .$$

Avec les significations suivantes :

1° B est un espace vectoriel à gauche sur son sous-anneau K, qui est un corps, et il existe $x \in B$, tel que x^j, $0 \leqslant j < n$, soit une base de B sur K, où on pose $x^0 = 1$, et où x^j est défini par récurrence avec $x^{j+1} = x \star x^j$;

2° $\forall\, a \in K$, $a \neq 0$, $\exists\, a_1 \in K$, $a_1 \neq 0$, $\exists\, a_2 \in K$, $x \star a = a_1 \star x + a_2$;

3° $\forall\, a$, $\forall\, b$, $\forall\, c \in K$, $i + j < n$, $k < n$, $[a \star x^i , b \star x^j , c \star x^k] = 0$ (associateur relatif à $\star$).

Les autres propriétés sont manifestement des conséquences de 3° :

4° $K \subset N_g \cap N_c$;

5° $1 \leqslant i < n$, $\forall\, b \in K$, $x^i \star b = x \star (x^{i-1} \star b)$;

6° i, j, k étant inférieurs à n, pour $i + j < n$, on a $[x^i , x^j , x^k] = 0$.

Pour établir (3), il suffit de prouver que (b) ==> (c), car (a) ==> (b) et (c) ==> (a) sont déjà prouvées. Pour cela, on prouve d'abord :

$$\forall\, a \in K , \qquad x \star a = \sigma(a) \star x + \delta(a) ,$$

où σ est un endomorphisme injectif de K, et δ une σ-dérivation de K. Il en résulte :

$$0 \leqslant p \leqslant k \leqslant n-1 , \qquad x^k \star a = \sum_{p=0}^{k-1} S_{k,p}(a) \star x^p .$$

En utilisant l'écriture de x^n sur la base, il est alors possible de calculer les produits $x^i \star x^j$ pour $1 \leqslant i < n$, $1 \leqslant j < n$. Grâce à 4°, la connaissance des produits $x^k \star a$ et $x^i \star x^j$ détermine la multiplication de B. Si on introduit A/Am selon (c), on constate que les produits $x^k.a$ et $x^i.x^j$ ont les mêmes valeurs, au changement de notations près, ce qui permet de prolonger l'isomorphisme évident pour les groupes additifs en un isomorphisme pour la multiplication.

Avec l'hypothèse supplémentaire $n = 2$, le résultat (3) donne :

(4) Tout anneau B à multiplication non nécessairement associative, qui est espace vectoriel à gauche de dimension 2 sur un de ses sous-anneaux K, avec $K \subset N_g \cap N_c$, est isomorphe à A/Am, avec d° $m = 2$.

On a obtenu avec 6° une propriété d'associativité restreinte sur les puissances de x , on peut préciser ce résultat ainsi :

(5) L'associativité pour la multiplication de toutes les puissances de x équivaut à $x^n.x = x.x^n$, ou à $mx \in Am$, ou encore à $x \in N_d$.

On donnera plus loin des exemples où cette associativité a lieu sans que A/Am ait une multiplication associative.

2. Propriétés de A/Am liées à la factorisation de m dans A .

Proposons-nous d'étudier l'équation en z : $z.a = b$, $a \neq 0$. Introduisons pour cela l'application D_a : $A/Am \to A/Am$, définie par $D_a(z) = z.a$. Compte tenu de 4°, on vérifie que D_a est une application K-linéaire, et comme A/Am est de dimension finie sur K , D_a est bijective si, et seulement si, $\operatorname{Ker} D_a$ est réduit à 0 . Or $u.a = 0$ équivaut à $ua \in Am$, donc

$$\operatorname{Ker} D_a = \{u \; ; \; u \in A_n \; , \; ua \in Am\} \; .$$

Mais dans A tous les idéaux à gauche sont de la forme Ar , donc on a

$$ua \in Am \iff ua \in Aa \cap Am = Af = Aha \; , \qquad \text{avec } d^\circ h = d^\circ f - d^\circ a \; .$$

Puisqu'on a $a \neq 0$, $ua \in Am$ équivaut à $u \in Ah$. Par suite, on a $\operatorname{Ker} D_a \neq 0$ si, et seulement s'il existe dans Ah un polynôme de degré strictement inférieur à n , ce qui équivaut à $d^\circ h \leqslant n - 1$. Or, dans A , il existe g tel que $Aa + Am = Ag$, et on a

$$d^\circ m - d^\circ g = d^\circ f - d^\circ a = d^\circ h \; .$$

Soit

$$d^\circ h \leqslant n - 1 \iff 1 \leqslant d^\circ g \; ;$$

g étant le p. g. c. d. à droite de a et m , on a :

(6) Pour $a \neq 0$, l'équation en z : $z.a = b$ admet une solution quel que soit b , si, et seulement si, le p. g. c. d. à droite de a et m est 1 , la solution est alors unique. $z.a = b$ admet une solution z pour tout $a \neq 0$ et pour tout b , si, et seulement si, m est irréductible dans A . Cette solution est alors unique pour a et b donnés.

Etudions l'équation analogue : $a.z = b$ pour $a \neq 0$. L'existence d'une solution z quel que soit b , équivaut à la surjectivité de l'application G_a définie par $G_a(z) = a.z$. Lorsque m est irréductible, G_a est injective, car $a.z = D_z(a) = 0$

est impossible pour $z \neq 0$, puisque D_z serait injective. Mais G_a n'étant pas en général K-linéaire, on ne peut pas toujours en déduire que G_a est surjective.

Soit L le sous-ensemble de K constitué par les éléments qui permutent avec tous les autres éléments de A/Am ; on peut montrer que L est un sous-corps commutatif de K , et que G_a est L-linéaire. Si m est irréductible, on peut aussi prouver que N_d est un corps gauche, et que G_a est N_d-linéaire, si on considère A/Am comme un espace vectoriel à droite sur N_d . Pour $\delta = 0$, on constate que la surjectivité de G_x exige σ surjectif. On en déduit :

(7) Le sous-ensemble L des éléments de K qui commutent avec tous les éléments de A/Am est un sous-corps commutatif de K , et A/Am est une algèbre sur L en général non associative. Si m est irréductible, N_d est un corps, et l'équation en z : $a.z = b$, $a \neq 0$, a au plus une solution. Pour qu'elle ait une solution pour tout $a \neq 0$ et tout b , il suffit d'avoir, soit $\dim_L$ A/Am finie, soit $\dim_{N_d}$ A/Am finie.

On peut tirer aussi de (5), en raisonnant sur les éléments inversibles de l'anneau N_d :

(8) Pour qu'il existe un sous-ensemble X de A/Am contenant toutes les puissances de x et ayant une structure de groupe pour la multiplication, il faut et il suffit que l'on ait

$$mx \in Am \qquad \text{et} \qquad m \notin Ax \ .$$

Ces conditions peuvent être réalisées avec m irréductible, sans que Am soit bilatère.

3. Caractérisation d'une classe de quasi-corps distributifs.

Parmi les algèbres A/Am obtenues, certaines sont particulièrement intéressantes pour l'étude des plans projectifs : ce sont les quasi-corps distributifs qui permettent de construire des plans de translation (voir [6], p. 92, pour définition). Nous savons déjà que A/Am est un anneau unitaire éventuellement sans associativité pour la multiplication. Pour obtenir un quasi-corps distributif, il faut et il suffit que A/Am ait une structure de boucle pour la multiplication, c'est-à-dire que M doit vérifier en outre :

M est fermé pour la multiplication .

Pour tout couple d'éléments a et b appartenant à M , il existe y et z

appartenant à M tels qu'on ait $a.y = b$, $z.a = b$.

Pour que M soit fermé pour la multiplication, il est nécessaire que m soit irréductible, en effet, sinon il existerait u et v dans A_n vérifiant $uv = m$, soit $u.v = 0$. Réciproquement, si m est irréductible, M est fermé, car $a \in M$, $b \in M$, $a.b = 0$ impliquerait l'existence de deux solutions $z = a \neq 0$ et $z = a$ pour l'équation $z.b = 0$, ce qui contredirait (6). Enfin, (6) et (7) donnent des conditions suffisantes pour l'existence et l'unicité des solutions de $z.a = b$ et $a.z = b$, pour a et b dans M . On vérifie facilement que ces solutions sont dans M . D'où, avec (1), il vient :

(9) Lorsque m est irréductible dans A , et que A/Am est de dimension finie comme espace vectoriel sur L , ou comme espace vectoriel à droite sur N_d , A/Am est un quasi-corps distributif. Ce quasi-corps est un corps si, et seulement si, Am est un idéal bilatère de A .

Avec (3) et (4), on obtient les caractérisations suivantes :

(10) Pour Q quasi-corps distributif, il y a équivalence entre les trois propriétés suivantes :

(a) Q vérifie 1°, 2°, 3° ;
(b) Q vérifie 1°, 2°, 4°, 5°, 6° ;
(c) Q est isomorphe à A/Am , avec

$$A = K[x , \sigma , \delta] , \qquad m = x^n - \sum_{p=0}^{n-1} m_p x^p ,$$

où σ et δ sont définies par :

$$\forall\, a \in K , \qquad x.a = \sigma(a).x + \delta(a) ,$$

. symbolisant la multiplication de Q , m étant irréductible dans A , et ses coefficients vérifiant

$$x^n = \sum_{p=0}^{n-1} m_p.x^p .$$

En particulier, tout quasi-corps distributif qui est espace vectoriel à gauche de dimension 2 sur K , sous-corps de $N_g \cap N_c$, est isomorphe à A/Am , selon (c), avec $n = 2$.

Pour approfondir l'étude de ces quasi-corps, il est utile d'obtenir d'autres résultats valables pour un A/Am quelconque. Remarquons que les règles de calcul dans

$A = K[x , \sigma , \delta]$ se simplifient beaucoup pour $\delta = 0$. En effet, on a alors

$$\forall\ a \in K , \quad \forall\ n \in \mathbb{N} , \qquad x^n\, a = \sigma^n(a) x \ .$$

Cette simplification se répercute dans A/Am , puisque, lorsque le degré d'un produit dans A est au plus égal à $n - 1$, il coïncide avec le produit dans A/Am .

Pour $r \in K$, $s \in K$, $r \neq 0$, posons $y = rx + s$, il est aisé de prouver que (y^i) , $0 \leqslant i \leqslant n$, est une K-base de A/Am . On montre alors que (10) s'applique, pour cette base, en vérifiant 1°, 2° et 3°, ce qui donne :

(11) Pour tout $r \in K$, $r \neq 0$, et pour tout $s \in K$, si on pose $y = r.x + s$, A/Am est isomorphe à $A'/A'm$, avec

$$A' = K[y , \sigma' , \delta'] , \qquad m' = y^n - \sum_{i=0}^{n-1} m'_i\, y^i \ ,$$

si y^n s'écrit

$$y^n = \sum_{i=0}^{n-1} m'_i . y^i \quad \text{dans} \quad A/Am \ ,$$

où σ' et δ' sont définies par

$$\forall\ a \in K , \qquad \sigma'(a) = r\sigma(a)\, r^{-1} \quad \text{et} \quad \delta'(a) = r\delta(a) + sa - r\sigma(a)\, r^{-1} s \ .$$

Un changement de base du type précédent permet de se ramener au cas où $\delta' = 0$ si, et seulement si, on peut trouver r et s dans K vérifiant, pour tout $a \in K$,

$$\delta(a) = r^{-1} sa - \sigma(a)\, r^{-1} s = ka - \sigma(a)k , \qquad \text{avec} \quad k = r^{-1} s \ ,$$

condition qui signifie que δ est une σ-dérivation intérieure (cf. [3], p. 171). On en déduit alors :

(12) Si δ est une σ-dérivation intérieure de K , il existe $k \in K$ tel que A/Am soit isomorphe à $A'/A'm$, avec

$$A' = K[y , \sigma , 0] \quad \text{et} \quad m' = (y - k)^n - \sum_{i=0}^{n-1} m_i (y - k)^i \quad \text{si} \quad m = x^n - \sum_{i=0}^{n-1} m_i\, x \ .$$

Ce dernier résultat prend tout son intérêt lorsqu'on prouve que certains corps n'admettent que les σ-dérivations intérieures comme σ-dérivations. On prouve alors :

(13) Tout corps commutatif K admettant une base de la forme (u^i), $0 \leqslant i \leqslant p > 1$, sur K_σ son sous-corps invariant élément à élément dans l'automorphisme σ de K, admet comme seules σ-dérivations les σ-dérivations intérieures.

Remarquons que ce résultat s'applique aux corps finis. Pour l'établir, on montre que l'espace vectoriel des σ-dérivations de K est de dimension 1 sur K.

4. Etude particulière du cas $\delta = 0$.

Si on suppose $\delta = 0$, ou si pour un corps n'admettant que des σ-dérivations intérieures on s'y ramène, certains problèmes sont plus faciles à traiter. On obtient, par exemple :

(14) Pour $\delta = 0$, les éléments de A/Am de la forme

$$c = \sum_{i=0}^{n-1} c_i . x^i \quad , \qquad \text{avec } \forall\, a \in K \ , \ 0 \leqslant i < n \ , \quad a c_i = c_i \, \sigma^i(a) \text{ et } \sigma(c_i) = c_i \ ,$$

commutent avec tous les autres. Lorsque x est inversible à gauche, ce sont les seuls.

On peut aussi caractériser les polynômes $m \in A$ tels que Am soit un idéal bilatère. Il suffit pour cela que l'on ait, $\forall\, a \in K$, $ma \in Am$ et $mx \in Am$, on en tire :

(15) Pour $\delta = 0$, les polynômes $m \in A$, tels que A/Am soit un anneau, sont caractérisés par les conditions :

Si $m = x^n - \sum_{i=0}^{n-1} m_i \, x^i$, pour $0 \leqslant i < n$, on a $\sigma^n(a) \, m_i = m_i \, \sigma^i(a)$ pour tout $a \in K$, et $\sigma(m_i) = m_i$.

Si les coefficients m_i sont dans le centre de K, si σ est d'ordre s, et si on a $n = rs + t$, $0 \leqslant t < s$, m est égal au produit d'un polynôme en x^s de degré r multiplié à droite par x^t.

On trouve aussi :

(16) Pour $\delta = 0$, on a $x \in N_d \iff m_i = \sigma(m_i)$, $\forall\, i$.

Avec (5), ces deux derniers résultats prouvent que l'associativité des puissances de x n'implique pas que A/Am soit un anneau, on pourra ainsi obtenir des quasi-corps où toutes les puissances de x s'associent sans avoir pour autant un corps.

Afin d'être en mesure de construire effectivement des quasi-corps, il faut disposer de polynômes irréductibles dans A. Signalons des cas particuliers où on peut en trouver assez commodément :

Si m est de degré 2, il est irréductible si, et seulement si, il n'admet pas de facteur du premier degré à droite. A l'aide d'une division, on obtiendra :

(17) Pour $\delta = 0$, $m = x^2 - m_1 x - m_0$ est irréductible si, et seulement si, on a

$$\forall\, t \in K, \qquad \sigma(t)t - m_1 t - m_0 \neq 0 .$$

Remarquons que, si K est un corps de Galois, la condition obtenue fait intervenir un polynôme ordinaire en t (noter que σ = identité, redonne la condition usuelle).

Si m, de degré 3, est réductible, il admet à gauche ou à droite un facteur de degré 1. On obtient :

(18) Pour $\delta = 0$, $m = x^3 - m_2 x^2 - m_1 x - m_0$ est irréductible si, et seulement si, on a

$$\forall\, t \in K \begin{cases} \sigma^2(t)\,\sigma(t)t - \sigma^2(t)\,\sigma(t)\,m_2 - \sigma^2(t)\,\sigma(m_1) - \sigma^2(m_0) \neq 0 , \\ \sigma^2(t)\,\sigma(t)t - m_2\,\sigma(t)t - m_1 t - m_0 \neq 0 . \end{cases}$$

Ces conditions prennent une forme particulièrement simple pour un corps de Galois.

De façon générale, on pourrait donner des c. n. s. pour m de degré n, en écrivant que m n'admet aucun facteur de degré $1, 2, \ldots, n-1$ à droite.

Avec une hypothèse supplémentaire sur K, on peut obtenir un résultat moins évident :

(19) Pour $\delta = 0$, n étant premier, ω désignant un élément du centre de K vérifiant

$$\sigma(\omega) = \omega , \quad \omega^k \neq 1 , \quad 0 \leqslant k < n , \quad \omega^n = 1 ,$$

le polynôme $x^n - a$ est irréductible dans $K[x, \sigma, 0]$ si, et seulement si, on a

$$\forall\, t \in K, \qquad a \neq \sigma^{n-1}(t)\,\sigma^{n-2}(t) \ldots \sigma(t)t \neq \sigma^{n-1}(a) .$$

(L'idée de cette démonstration provient de l'exercice n° 8, de [1], p. 148.)

5. Application à l'étude des quasi-corps distributifs finis.

Dans le cas où K est un corps fini, les résultats obtenus se simplifient pour deux raisons essentielles :

- On peut toujours se ramener au cas où $\delta = 0$ par un changement de base ;
- A/Am est toujours de dimension finie sur L et sur N_d .

Grâce à (10), (9), (5), et (15), on obtient en définitive :

(20) Pour tout quasi-corps distributif fini, il y a équivalence entre (a), (b), (c) :

(a) Q vérifie 1°, 2°, 3° ;
(b) Q vérifie 1°, 2°, 4°, 5°, 6° ;
(c) Q est isomorphe à A/Am , avec

$$A = K[x\ ,\ \sigma\ ,\ 0]\ , \qquad m = x^n - \sum_{p=0}^{n-1} m_p\, x^p\ ,$$

où m est irréductible dans A , et a ses coefficients qui vérifient

$$x^n = \sum_{p=0}^{n-1} m_p . x^p\ .$$

Pour tout polynôme irréductible m de $A = K[x\ ,\ \sigma\ ,\ 0]$, A/Am est un quasi-corps distributif, dans lequel les puissances de x constituent un groupe multiplicatif si, et seulement si, on a, pour $0 \leqslant p \leqslant n-1$, $\sigma(m_p) = m_p$. On obtient un corps si, et seulement si, outre cette dernière condition, on a aussi

$$m = (x^s)^r - \sum_{j=0}^{r-1} m_j (x^s)^j\ ,$$

où s désigne l'ordre de σ .

Il est facile d'utiliser (17) et (18) pour construire effectivement des quasi-corps de dimension 2 et 3 sur K . Pour utiliser (19), on établit d'abord une propriété de certains idéaux d'un anneau unitaire, qui fournit dans le cas de Z une généralisation d'un théorème d'arithmétique :

(21) p désignant un élément du centre d'un anneau unitaire A , a et b deux entiers positifs, on a

$$(p^a - 1) + (p^b - 1) = (p^{a \wedge b} - 1)\ ,$$

où on désigne par (x) l'idéal bilatère de A engendré par $x \in A$.

La démonstration utilise l'algorithme permettant de calculer $a \wedge b$ à partir de a et b par divisions successives, pour en déduire une écriture convenable de $1 + \sum_{k=1}^{k=a} p^k$.

On peut alors déduire de (19) et (21) :

(22) K désignant le corps de Galois d'ordre p^r , σ désignant son automorphisme défini par

$$\sigma(y) = y^{p^s} , \qquad s \neq 0 , \quad \forall\, y \in K ,$$

z engendrant le groupe multiplicatif de K , n étant un diviseur premier de $p^{s \wedge r} - 1$, il existe $a \in K$ tel que $A/A(x^n - a)$, avec $A = K[x , \sigma , 0]$, soit un quasi-corps distributif si, et seulement si, on a

$$(p^r - 1)(p^s - 1) \wedge (p^{ns} - 1) > p^s - 1 .$$

Alors, $A/A(x^n - a)$ n'est pas un corps, et les $a \in K$ ayant cette propriété sont ceux qui s'écrivent $a = z^u$, avec $u \notin Z(p^{ns} - 1)(p^s - 1)^{-1}$.

Pour $n = 2$ et $n = 3$, l'hypothèse " n divise $p^{s \wedge r} - 1$ " est superflue.

Il est possible de donner des conditions suffisantes plus simples qui permettent d'appliquer (22), par exemple, pour les valeurs

$$(p , n) = (11 , 5) , (29 , 7) , (67 , 11) , \ldots$$

qui ont en commun la propriété $p \equiv 1 \pmod{n}$, avec r multiple de n .

Enfin, pour $p = 11$, $r = 2$, $s = 1$, et $n = 5$, il suffit de prendre $a = z^{12}$ pour obtenir un exemple de quasi-corps fini, qui n'est pas un corps, et où cependant les éléments x^i de la base engendrent un groupe multiplicatif (on utilise (17), (21) et $Z/5^2 Z$.

Nos résultats généralisent effectivement certains résultats :

Dans [7], SANDLER considère une classe d'algèbres non associatives de dimension finie sur un corps de Galois K , où intervient un automorphisme σ de K . On montre que ces algèbres sont des algèbres A/Am , avec

$$A = K[x , \sigma^{-1} , 0] \qquad \text{et} \qquad m = x^n - a ,$$

lorsqu'on a $\sigma^n = \text{identité}$. Le dernier exemple ci-dessus n'est pas de ce type, en effet l'ordre de σ $(= 2)$ ne divise pas $n = 5$.

Dans [2], HUGHES et KLEINFELD caractérisent un type de quasi-corps finis de dimen-

sion 2 sur un corps de Galois. Grâce en particulier à (10), on retrouve leurs résultats. On retrouve aussi une partie d'un théorème de KNUTH ([4], p 215) qui leur est apparenté.

6. Application à la construction de quasi-corps distributifs infinis.

Soulignons les principales différences qui distinguent ce cas du précédent :

- Il n'y a pas que le cas où $\delta = 0$ qui soit à considérer, puisque, si on prend par exemple pour K un corps de fractions rationnelles à coefficients dans un corps commutatif, avec σ = identité , et pour δ la dérivation usuelle des fractions rationnelles, on obtient une σ-dérivation qui n'est pas une dérivation intérieure.

- L'irréductibilité de m , si elle assure toujours l'existence et l'unicité de la solution z de $z.a = b$ pour $a \neq 0$, ne suffit pas pour que A/Am soit un quasi-corps. On peut le prouver à l'aide d'un exemple où K est un corps de fractions rationnelles à coefficients dans un corps commutatif, et où σ est un isomorphisme non surjectif de K . Pour avoir un quasi-corps, il suffira de montrer en outre que A/Am est de dimension finie sur L à gauche, ou sur N_d à droite, ou sur K à droite, ce qui est vrai quand σ est surjectif.

- Etant infini, A/Am pourra être un corps non commutatif, même si K est commutatif.

- Si K n'est pas commutatif, on pourra obtenir des quasi-corps non associatifs, avec σ = identité et $\delta = 0$.

Commençons par remarquer que, d'après (17), (9) et (15), le polynôme $x^2 + 1$ est irréductible dans $K[x , \sigma , 0]$, lorsque K est le corps des nombres complexes et σ son automorphisme involutif, et $A/A(x^2 + 1)$ est un corps non commutatif, puisque σ n'étant pas l'identité, on a $x.a \neq a.x$ en général. On reconnaît le corps des quaternions.

Lorsque K est commutatif, (17) et (18) permettent d'obtenir, avec des hypothèses supplémentaires, des résultats qui sont d'ailleurs valables dans le cas fini :

(23) K étant un corps commutatif ayant un automorphisme σ d'ordre 2 , si on a $m_1 \neq 0$, $\sigma(m_1) = m_1$, $\sigma(m_0) = m_0$, et $A = K[x , \sigma , 0]$, il y a équivalence entre :

(a) $A/A(x^2 - m_1 x - m_0)$ est un quasi-corps distributif ;
(b) $t^2 - m_1 t - m_0$ n'a pas de racine invariante par σ .

Ce quasi-corps n'est pas associatif, et les puissances de x constituent un groupe multiplicatif.

(24) K étant un corps commutatif ayant un automorphisme σ d'ordre 2, si on a m_0, m_1, m_2 invariants par σ et $m_1 m_2 + m_0 \neq 0$, pour $m = x^3 - m_2 x^2 - m_1 x - m_0$ et $A = K[x, \sigma, 0]$, il y a équivalence entre :

(a) A/Am est un quasi-corps distributif ;

(b) $t^3 - m_2 t^2 - m_1 t - m_0$ n'a pas de racine invariante par σ.

Le quasi-corps obtenu n'est pas associatif, et les puissances de x constituent un groupe multiplicatif.

Exemple d'applications. - Si on prend pour K le corps des nombres complexes, et pour m le polynôme $t^2 + t + t$, avec $\sigma(z) = \bar{z}$, $\forall\, z \in K$, on obtient un quasi-corps qui généralise d'une certaine façon le corps des quaternions.

Si on prend pour K le sous-corps des nombres complexes de la forme $a + ib$, $a \in Q$, $b \in Q$, avec $\sigma(a + ib) = a - ib$, et $m = x^3 - 2$, on obtient un quasi-corps dans lequel (14) permet de montrer que le sous-ensemble des éléments commutant avec tous les autres n'est pas fermé pour la multiplication.

On pourrait aussi appliquer (19) à un corps contenant un corps cyclotomique comme sous-corps.

Lorsque K n'est pas commutatif, il est très facile de voir ce que donne (17) pour σ-identité. On obtient ainsi l'exemple suivant :

K étant le corps des quaternions sur Q, on sait qu'il existe une base (e_i), $0 \leqslant i \leqslant 3$, et une norme N définie par

$$N(y) = \sum_{i=0}^{i=3} y_i^2 \qquad \text{pour} \quad y = \sum_{i=0}^{i=3} y_i\, e_i\,, \quad y_i \in Q\,.$$

Si on prend $m_1 = 0$, $m_0 = 1 + e_1$, on obtient un quasi-corps dans lequel x n'appartient pas à N_d.

Si on impose en outre que m_1 et m_2 appartiennent au centre de K, alors (18) prend une forme particulièrement simple qui permet d'obtenir l'exemple suivant :

Pour le choix de corps et d'automorphisme précédent, on obtient un quasi-corps distributif où x n'appartient pas à N_d, en prenant $m = x^3 - 1 - e_1$. Enfin, si dans cet exemple, on remplace $1 + e_1$ par 2, on obtient un corps gauche.

Pour appliquer (19), considérons le sous-corps L du corps des quaternions réels engendré par les quaternions à coefficients rationnels, et z une racine n-ième de l'unité pour n entier premier (il en existe dans le corps des complexes, donc aussi dans celui des quaternions réels), (19) donne alors :

(25) $L[x]/L[x](x^n - r)$ est un quasi-corps distributif si, et seulement si, on a $r \neq t^n$, $\forall\, t \in L$. C'est un corps si, et seulement si, r est dans le centre de L .

On remarque que $N(r) \neq N(t)^n$ suffit pour avoir $r \neq t^n$.

7. Application à l'étude des corps gauches de dimension finie sur leur centre.

Nous avons vu que certains choix permettent d'obtenir des corps gauches A/Am . En utilisant des résultats connus de la théorie des corps gauches de dimension finie sur leur centre, on arrive à une caractérisation des corps gauches, lesquels peuvent se construire à partir d'un de leur sous-corps commutatif maximal par une suite d'extensions successives du type extension de K à $A/A(x^n - a)$, où $A = K[x\ ,\ \sigma\ ,\ 0]$.

Soit un corps gauche de dimension finie sur son centre C , soit G le groupe des automorphismes de M qui conservent les éléments de C . Adoptons désormais les notations suivantes : y^σ au lieu de $\sigma(y)$, et $\tau\sigma$ au lieu de $\sigma \circ \tau$. En utilisant le fait que tout automorphisme de G peut être prolongé en un automorphisme intérieur de K , et que la dimension de K sur M est égale à celle de M sur C , on prouve dans l'ordre :

(26) Pour tout élément $\sigma \in G$, il existe $x_\sigma \in K$ tel que la restriction à M de l'automorphisme intérieur $y \to x_\sigma^{-1} y x_\sigma$ soit σ , et le sous-ensemble de K dont les éléments ont cette propriété est $M^* x_\sigma$, avec $M^* = M - \{0\}$. Le sous-ensemble des parties de K , $\{M^* x_\sigma\ ,\ \sigma \in G\}$, est un groupe isomorphe à G pour la loi $M^* x_\sigma M^* x_\tau = M^* x_{\sigma\tau}$, σ et $M^* x_\sigma$ se correspondant dans cet isomorphisme.

(27) Il existe un sous-corps $M(G)$ de K admettant comme base sur M , (x_σ) , $\sigma \in G$. La multiplication de $M(G)$ est définie par la connaissance des constantes $a_{\sigma,\tau} \in M$, avec les règles

$$x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau} \qquad \text{et} \qquad y x_\sigma = x_\sigma y^\sigma\ ,\quad \forall\, y \in M\ ,\quad \forall\, \sigma \in G\ .$$

K est égal à $M(G)$ si, et seulement si, M est extension galoisienne de C . A tout sous-groupe H de G correspond un sous-corps $M(H)$ de $M(G)$, de base (x_σ) , $\sigma \in H$, sur M .

Dans le cas où H est un sous-groupe cyclique d'ordre h , la structure de $M(H)$ est déterminée par le résultat suivant :

(28) Pour tout sous-groupe cyclique H de G d'ordre h, engendré par σ, il existe $a \in M$ invariant par σ, tel que M(H) soit isomorphe à $A/A(x^h - a)$ pour $A = M[x, \sigma, 0]$.

Grâce à (26), on peut caractériser les sous-corps M(H), H sous-groupe de G, qui sont invariants dans l'automorphisme intérieur associé à x_τ. Compte tenu du résultat précédent, il est possible de prouver le résultat essentiel suivant :

(29) Il y a équivalence entre (a) et (b) :

(a) Il existe une suite de corps M_k, $0 \leqslant k < s$, vérifiant :

$$M = M_0 \subset M_1 \subset \ldots \subset M_k \subset M_{k+1} \subset M_s = M(G) \quad ,$$

avec

$$M_{k+1} \approx M_k[x, \tau_{k+1}, 0]/(x^{q_k} - c_k) \qquad \text{pour } 0 \leqslant k < s \quad ,$$

où τ_{k+1} est un automorphisme de M_k qui induit sur M l'automorphisme $\sigma_{k+1} \in G$;

(b) Le groupe G est résoluble.

Remarquons que ce résultat ressemble à un théorème concernant la résolution, par radicaux, d'une équation à coefficients dans un corps commutatif (on peut même se ramener au cas où les q_k sont des nombres premiers).

Avec (27), (29) permet de caractériser la structure des corps gauches, de dimension finie sur leur centre, qui possèdent un sous-corps commutatif maximal, extension galoisienne à groupe de Galois résoluble de ce centre.

BIBLIOGRAPHIE

[1] BOURBAKI (Nicolas). - Algèbre. Chap. 8 : Modules et anneaux semi-simples. - Paris, Hermann, 1958 (Act. scient. et ind. 1261 ; Bourbaki, 23).

[2] HUGHES (D. R.) and KLEINFELD (E.). - Seminuclear extensions of Galois fields, Amer. J. of Math., t. 82, 1960, p. 389-392.

[3] JACOBSON (Nathan). - Structure of rings. - Providence, American mathematical Society, 1956 (American mathematical Society. Colloquium Publications, 37).

[4] KNUTH (Donald E.). - Finite semifields and projective planes, J. of Algebra, t. 2, 1965, p. 182-217.

[5] ORE (Oystein). - Theory of non-commutative polynomials, Annals of Math., Series 2, t. 34, 1933, p. 480-508.

[6] PICKERT (Günter). - Projektive Ebenen. - Berlin, Springer-Verlag, 1955 (Die Grundlehren der mathematischen Wissenschaften, 80).

[7] SANDLER (R.). - Autotopism groups of some finite non-associative algebra, Amer. J. of Math., t. 84, 1962, p. 239-264.

N.-B. - Il est possible que les résultats présentés dans cet exposé fassent l'objet d'une publication ultérieure de l'auteur.